Montana Law Review

Volume 72
Issue 2 *Summer 2011*

Article 3

7-2011

Is the Government in My Pocket? An Overview of Government Location Tracking of Cell Phones Under the Federal System and in Montana

Briana Schwandt
University of Montana School of Law

IS THE GOVERNMENT IN MY POCKET? AN OVERVIEW OF GOVERNMENT LOCATION TRACKING OF CELL PHONES UNDER THE FEDERAL SYSTEM AND IN MONTANA

Briana Schwandt*

"Subtler and more far-reaching means of invading privacy have become available to the government. . . . The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping."

Justice Brandeis[1]

I. INTRODUCTION

Most Americans love the convenience of having a cell phone. We carry them around in our pockets, our purses, and our backpacks. We can make calls, receive calls, text message, browse the Internet, and receive directions at the drop of a dime right from our phones. What most of us do not know is that even if our phones are not enabled with global positioning system ("GPS") technology, they can be tracked. A disturbing trend has arisen in which law enforcement agencies obtain cell phone records without subscribers' knowledge or consent, sometimes without the authority of a neutral and detached judge. Law enforcement uses the records not only to determine where subscribers have been, but also to track them in real time. Essentially, cell phones are capable of being used as personal tracking devices that can monitor a subscriber's every move. The only way subscribers can prevent tracking is to turn off their phones.

Federal laws governing electronic monitoring are sorely outdated. Adding to the confusion, federal courts apply these outdated statutes with differing outcomes, leaving practitioners without clear guidance on how to approach this growing trend. The very nature of the record request proceedings has resulted in little precedent for courts to follow. After all, when the government seeks permission to obtain records, it does so without informing the target. Therefore, there is no defendant when a court grants the request. And when the request is denied, the federal or state government does not appeal. In Montana, neither the Legislature nor the courts have

* Briana Schwandt, Student Author, graduated from the University of Montana School of Law in the Spring of 2011. The author would like to thank Betsy Griffing for all her encouragement and help with this article.

1. *Olmstead v. U.S.*, 277 U.S. 438, 473–474 (1928) (Brandeis, J., dissenting), *overruled*, *Katz v. U.S.*, 389 U.S. 347, 353 (1967).

addressed the particular issue of cell phone location tracking, forcing practitioners to invent creative arguments to deal with possible violations of their clients' rights.

Although most searches of cell phone subscribers' records are a necessary tool for law enforcement, this technology has significant potential for abuse. To ensure that neither federal nor state constitutional rights are infringed, law enforcement should be required to obtain a search warrant based on probable cause to receive these personal and revealing records. Without such a showing, the constitutional rights of Montana citizens are compromised, and the intentions of the 1972 Montana Constitution's drafters are blatantly disregarded.

This article provides an overview of federal and Montana law on the topic of cell phone location tracking and is intended to raise awareness about the government's ability to locate individuals through that technology. It does not attempt to describe the technology in detail, but merely to provide a broad understanding. The article focuses on how the law is dealing with this technology as it collides with citizens' right of privacy and the requirements of search and seizure under federal and Montana law.

Section II of this article provides a general overview of the basics of cell phone location tracking technology,[2] its possible constitutional implications under the federal Constitution, and the current federal laws that govern electronic monitoring. Section III discusses federal case law interpreting the federal statutes and concerning electronic monitoring in general. Section IV provides a detailed discussion of the transcripts of the 1972 Montana Constitutional Convention and Montana case law pertinent to the discussion of cell phone location tracking. Finally, Section V explores the legal trend of location tracking jurisprudence and provides a conclusion about the practice in Montana.

II. Overview of Cell Phone Location Tracking

Anytime a cell phone is turned on, even if the phone is not being used to make or receive a call, it can be located. This is possible because of a process called "registration."[3] To maintain the strongest signal, the phone searches for the nearest tower every seven seconds.[4] The data generated during registration contains no communication; it only identifies the towers to and from which the phone is sending and receiving signals.[5] Cell phone

2. For a more detailed description of this technology, see *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005).

3. Timothy Stapleton, *The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More Than the Sum of Its Parts?*, 73 Brook. L. Rev. 383, 387 (2007).

4. *Application for Pen Register*, 396 F. Supp. 2d at 750.

5. Stapleton, *supra* n. 3, at 387.

service providers store all of this data.[6] Although no communications are involved, this information allows law enforcement to determine the location of the cell phone and, hence, the location of the cell phone's owner. Because no communications are involved with these transmissions, attempts by law enforcement to access this data have raised differences in interpretation by courts of Fourth Amendment search and seizure requirements, statutory requirements, and the right of privacy.

Registration information can be divided into real-time and historical data. On the one hand, real-time data allows the government to track the current whereabouts of a suspect.[7] On the other hand, historical data allows the government to determine the whereabouts of a suspect at a previous point in time by looking at the service provider's stored records.[8] Law enforcement can use real-time data to find a fugitive or even a kidnapping suspect. In one situation, a victim's phone was in her car when it was stolen, and the phone was used to track the whereabouts of the stolen car and suspect.[9] Historical data can be used to corroborate or disprove a suspect's alibi, as it was used to disprove Scott Peterson's alibi and help convict him of the murder of his wife, Lacey Peterson.[10]

Although these illustrations provide examples where this information was used to produce positive results, the use of this information is potentially subject to great abuse when not checked by a neutral judiciary.

The government has several methods to access cell phone users' locations. The Federal Communications Commission ("FCC") has mandated

---

6. *In re Application of U.S. for an Or. Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. (Sealed)*, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

7. *Id.* at 598.

8. Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 Hastings Comm. & Ent. L.J. 421, 431–432 (2007).

9. *See* Stapleton, *supra* n. 3, at 383–384. "In one case, a thief stole a woman's car with her child and her cell phone inside. The police were able to stop the car and rescue the child within thirty minutes by tracking the woman's cell phone." *Id.* (citing *Girl, 5, Found Safe as Man Steals Car*, Rocky Mt. News A18 (Apr. 22, 2004). *See* Lockwood, *infra* n. 18, at 310. "Throughout his journey, U.S. marshals tracked his movements by monitoring his cell phone usage until a police officer recognized the rented vehicle and began a high-speed pursuit that ended with the suspect's capture." *Id.* (citing Don Plummer, *Cellphone Betrays Cobb Fugitive*, Atlanta J. Const. A1 (Nov. 9, 2003).

10. *See* Stapleton, *supra* n. 3, at 383. "In California, the evidence used to convict Scott Peterson of murdering his wife included location data gleaned from his cell phone that undermined his alibi." *Id.* (citing Diana Walsh & Stacy Finz, *The Peterson Trial: Defendant Lied Often, Recorded Calls Show Supporters Misled About Whereabouts*, S.F. Chron. B1 (Aug. 26, 2004); *see also* Lockwood, *infra* n. 18, at 310–311. "[H]e told police he was not in the area at the time of the murder. However, cell phone records proved otherwise. The cell tower information for his calls placed him within blocks of the scene of the crime both before and three minutes after the shooting. Records further indicated that during the actual murder, he likely had the phone turned off. Prosecutors argued this was also inculpatory in that someone who was secretly stalking a victim would not want a cell phone call to alert the victim to his presence." *Id.* (citing Holley Gilbert, *Vancouver Man is Arrested in Shooting Death of Ex-Girlfriend*, Portland Oregonian B1 (Apr. 30, 2004)).

implementation of a system whereby 911 operators are able to determine the location of callers from their cell phones. This system has increased the availability of and ease with which location data can be gathered by law enforcement. The methods for obtaining location data include Global Positioning System ("GPS") technology, Time Difference of Arrival ("TDOA"), and Angle of Arrival ("AOA"). Each method will be explored in turn.

With the advent of cell phones, 911 operators were alarmed they could not determine the location of distressed cell phone callers. To combat this problem and ensure the viability of the 911 emergency system, the FCC began issuing regulations in 1996 to ensure 911 operators could locate the callers through cell service providers' records. These regulations require service providers to make this information available to 911 operators.[11] The FCC also established a December 31, 2005 deadline for service providers to implement the necessary equipment and personnel to supply 911 operators with a caller's location within 150 meters.[12] The service providers typically use one of three methods to determine the cell phone's location. The methods include GPS technology, TDOA, or AOA. Although other methods exist, such as single cell site data, these three methods are the most accurate and the only three that will be discussed.

GPS only works on cell phones enabled with GPS technology. GPS is accurate in providing a cell phone's location within 10 to 20 meters as long as no obstructions like trees or tall buildings interfere with the signal.[13] GPS-enabled cell phones contain a GPS receiver that receives signals transmitted from several satellites, which indicate each satellite's location and the current time.[14] At least 24 GPS satellites are in the sky at all times.[15] When a cell phone's GPS receiver obtains information from at least four of these satellites, the receiver can estimate the distance to each satellite and calculate the phone's position in three dimensions.[16] GPS technology is becoming more popular in cell phones so that their users are able to enjoy navigation functions, turn-by-turn directions, and even track family mem-

11. 47 C.F.R. § 20.18(b) (2008).

12. 47 C.F.R. § 20.18 (2004) (requiring service providers to "achieve 95 percent penetration of location-capable handsets among its subscribers" by December 31, 2005). To learn more about the requirements of the different phases of this legislation, see Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 Rich. J.L. & Tech. 16 (Spr. 2007).

13. Smithsonian Natl. Air & Space Museum, *How Does GPS Work?*, http://www.nasm.si.edu/exhibitions/gps/work.html (last accessed March 21, 2011).

14. *Id.*

15. *Id.*

16. *Id.* For more detailed information on how this technology works, see Smithsonian Natl. Air & Space Museum, *GPS in More Detail*, http://www.nasm.si.edu/exhibitions/gps/spheres.html (last accessed March 21, 2011).

bers directly from their phones. Thus, more cell phone users can now be tracked through GPS technology.

Even if a person does not have a GPS-enabled cell phone, he or she can still be located through the use of signal triangulation. Signal triangulation uses the service providers' cell towers to obtain location information or "cell site data." Triangulation can be achieved through TDOA or AOA.

Time Difference of Arrival ("TDOA") is a system that enables the service provider to determine the cell phone's longitude and latitude either during registration[17] or when a call is made or received. This requires cell phone towers to estimate the time it takes the tower's signal to reach the cell phone or vice versa. With these estimates, the tower can determine the distance of the cell phone from the tower and, if more than one tower receives a signal, "an algorithm allows the system to determine coordinates corresponding to the phone's latitude and longitude."[18]

Angle of Arrival ("AOA") is similar to TDOA in that it uses signals between cell towers and cell phones. However, rather than measuring the amount of time a signal takes to travel from the cell phone to the tower, AOA technology enables the tower to record the angle of the signal as it arrives at the tower.[19] When more than one tower receives the signal, the differences in the angles of arrival are compared (triangulated) to determine the relative location of the cell phone.[20]

In rural settings with fewer towers, like in Montana, the location information provided by triangulation may be significantly less accurate. This occurs simply because fewer towers exist with which comparison of the cell signals' angles or distances can be achieved. When only a single tower exists to cover several hundred miles, neither the TDOA nor the AOA methods will work.[21] However, GPS technology still functions.

III. Federal Constitutional and Statutory Implications

Cell phone tracking technology has outgrown traditional constitutional and statutory analysis: "When new technology emerges, the first applications of the law try to build on old paradigms, generally without contemplating whether the new tools challenge the implicit assumptions of the past."[22] The drafters of the federal statutes that govern other types of sur-

17. Recall that registration is the process whereby the cell phone emits signals every seven seconds to find the closest tower and ensure the highest quality calls.

18. Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J.L. & Tech. 307, 308–309 (2004).

19. *Id.* at 309.

20. *Id.*

21. *Id.* at 309–310.

22. Ian James Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. Rev. 1324, 1328 (2008).

veillance simply did not contemplate cell phone location tracking. Thus, federal district court interpretations of these statutes as applied to requests for cell site data have produced mixed results.

A. *Federal Constitutional Implications*

The two most obvious constitutional rights triggered by law enforcement's use of cell phone location tracking are a citizen's Fourth Amendment right against unreasonable searches and seizures and a citizen's right of privacy. Courts have had to determine if the practice of obtaining cell site data records, whether historical or real-time, constitutes a search under the Fourth Amendment and whether cell phone users have a right of privacy in the cell phone records held by third-party service providers. Since this is such a new area of the law, practitioners have not yet developed constitutional arguments as has been done with pen registers and trap and trace devices.[23] Parties have argued additional constitutional implications in cases dealing with these similar but older technologies, and with the proper facts, the arguments might be utilized in the area of cell phone location tracking as well.

The rights of association, free speech, and a free press are also potentially implicated in cell phone location tracking. As with the pen register, trap and trace, and wiretap cases, some argue that tracking an individual's location through a cell phone violates the right of association.[24] In *O'Neal v. United States*, the Internal Revenue Service issued a summons to the telephone company requesting its toll records for the previous six months and that the telephone numbers identified on the toll records include the names and addresses of the holders.[25] The plaintiff-subscriber argued that including this information amounted to a compelled disclosure of his association's membership list and that the revelation of this list would have a chilling effect on his right of association.[26] Although this argument did not persuade the court, the right of association can be bolstered with the freedom of speech. In *NAACP v. Alabama*,[27] the United States Supreme Court held that freedom of association is an essential part of the freedom of

23. A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted . . . ." 18 U.S.C. § 3127(3) (2006). A trap and trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . " 18 U.S.C. § 3127 (4).

24. *See O'Neal v. U.S.*, 601 F. Supp. 874 (N.D. Ind. 1985).

25. *Id.* at 875–876.

26. *Id.* at 876. The court held that the plaintiff-subscriber failed to show compelled disclosure and consequences objectively suggesting an impact on the members' associational rights. *Id.* at 878–880.

27. *NAACP v. Ala. ex. rel Patterson*, 357 U.S. 449 (1958).

speech because people often cannot engage in effective speech unless they join with others.[28] The Court also held that the Constitution affords these rights to state citizens against state governments through the Due Process Clause of the Fourteenth Amendment.[29] Another possible constitutional implication might be the government's violation of a journalist's freedom of press under the First Amendment. Cell phone location tracking may reveal sensitive information about the identity and location of a journalist's source of information on a sensitive story and may therefore interfere with a journalist's ability to gather news.[30]

B. Federal Statutory Implications

Several federal statutes deal with how and when the government may use surveillance devices such as pen registers and trap and trace devices. None of these statutes specifically deal with cell phone location tracking. Nonetheless, the Wiretap Act, the Electronic Communications Privacy Act, Communications Assistance for Law Enforcement Act, and the Mobile Tracking Device Statute are particularly relevant.

The "Wiretap Act" is Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[31] The Act sets forth strict procedural requirements for law enforcement to follow when intercepting wire communications and prohibits public parties from intercepting any covered communications.[32]

After the advent of electronic mail and cell phones, Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA") to deal with these new technologies.[33] Title I of the ECPA generally extends the protections of the Wiretap Act to electronic communications. However, it specifically exempts electronic communications from the statutory suppression remedies available to wire or oral communications under the Wiretap Act while leaving Fourth Amendment remedies intact.[34] Title I also includes language regarding mobile tracking devices.[35] Title II, commonly referred

28. *Id.* at 460–461.

29. *Id.*

30. *See Rptrs. Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F. 2d 1030, 1046–1047 (D.C. 1978).

31. Pub. L. No. 90–351, § 802, 82 Stat. 197, 212–223 (1968) (codified at 18 U.S.C. §§ 2510–2520).

32. *Id.* The Wiretap Act will not be discussed in any greater detail because of its limited relevance to cell phone location tracking. *See U.S. v. Forest*, 355 F.3d 942, 948–949 (2004).

33. Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 1367, 2521, 2701–2711, 3117, 3121–3127).

34. *See* 18 U.S.C. §§ 2518(10)(a), (c); *U.S. v. Gbemisola*, 225 F.3d 753, 759 (D.C. Cir. 2000) (stating § 3117 does not specifically prohibit installation that does not conform to the statute and that violation of the statute does not result in exclusion of evidence unless the Fourth Amendment is also violated during installation).

35. Pub. L. No. 99–508, § 108(a), 100 Stat. 1848, 1858 (1986) (codified at 18 U.S.C. § 3117).

to as the "Stored Communications Act" ("SCA"), protects stored communications and transactional records.[36] Title III, the "Pen Register Act," deals with pen registers and trap and trace devices.[37]

In 1994, Congress passed the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").[38] This Act enumerates telecommunications carriers' obligations to help law enforcement intercept digital communications.[39]

Title I of the ECPA, the Mobile Tracking Device Statute, defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[40] To install a tracking device, the government must get a warrant or other order from a court in the jurisdiction in which the device will be installed.[41] This statute specifically allows the use of the device in other jurisdictions as long as it was installed in the jurisdiction in which the court order or warrant was issued.[42] An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ."[43] Although the signal produced by the tracking device would seem to qualify as an electronic communication, the definition specifically excludes the signals produced by tracking devices.[44] Because of this exclusion, the statutory requirements of the ECPA do not apply to cell site data and an individual cannot rely on their protections.

Under the Stored Communications Act, Title II of the ECPA, government agencies must follow a complicated statutory scheme to obtain electronically stored transactional records and communications. Electronically stored communications are those "communications obtained in a manner not simultaneous with their transmission."[45] Under the Act, stored records are identified as communications stored less than 180 days, communications stored more than 180 days, or transactional or subscriber informa-

36. Pub. L. No. 99–508, § 201(a), 100 Stat. 1848, 1860 (1986) (codified at 18 U.S.C. §§ 2701–2711).

37. Pub. L. No. 99–508, § 301(a), 100 Stat. 1848, 1868 (1986) (codified at 18 U.S.C. §§ 3121–3127).

38. Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010).

39. 47 U.S.C. § 1002(a)(2).

40. 18 U.S.C. § 3117(b).

41. *Id.* at § 3117(a).

42. *Id.*

43. *Id.* at § 2510(12).

44. *See* 18 U.S.C. § 2510(12)(C) (the signal an electronic device produces is not to be considered an "electronic communication," and so the statutory requirements of the ECPA do not apply).

45. Toeniskoetter, *supra* n. 12, at 8.

tion.[46] If the communications have been stored less than 180 days, the government needs a warrant in compliance with the Federal Rules of Criminal Procedure to obtain them.[47] If the communications are more than 180 days old, the government may obtain them in one of three ways. First, it may obtain the communications through a warrant in compliance with the Federal Rules of Criminal Procedure without having to give notice to the subscriber.[48] Second, if the government gives notice to the subscriber, it may obtain the communications by an administrative subpoena authorized by law or a grand jury, or by a trial subpoena.[49] Third, the government can obtain a court order for the records after making a showing to a court that it has "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[50] The entity may obtain transactional information by obtaining a warrant that complies with the Federal Rules of Criminal Procedure by making a probable cause showing or by obtaining a court order as described above.[51]

The Pen Register Act regulates when and how the government may install pen registers and trap and trace devices.[52] A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted . . ."[53] The definition specifically excludes content of any communication, device, or process used by the provider for billing, cost accounting, or other similar purposes in the ordinary course of business.[54] A trap and trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . . ."[55] This definition also excludes specifically the content of communications.[56] Unlike some of the requirements for obtaining stored information, the entity is not required, under any circum-

46. 18 U.S.C. § 2703. *See also* Toeniskoetter, *supra* n. 12, at 9.

47. *Id.* at § 2703(a).

48. *Id.* at § 2703(b)(A).

49. *Id.* at § 2703(b)(B)(i).

50. *Id.* at § 2703(b)(B)(ii), (d).

51. *Id.* at § 2703(c)(1)(A)–(B), (d). The entity may also obtain the records with the consent of the subscriber, or in certain circumstances involving telemarketing fraud. 18 U.S.C. § 2703 (c)(1)(C)–(D).

52. 18 U.S.C. §§ 3121–3127.

53. *Id.* at § 3127(3).

54. *Id.*

55. *Id.* at § 3127(4).

56. *Id.*

stances, to give notice to the subscriber.[57] As long as a court receives an application from a law enforcement officer or United States Attorney who has certified "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation" and the application is otherwise complete, the court must grant the application.[58]

CALEA enables law enforcement agents to "access call-identifying information that is reasonably available to the carrier . . . before, during or immediately after the transmission of a wire or electronic communication . . . ."[59] The statute narrows the scope of "call-identifying information" that carriers are required to provide when law enforcement is authorized only to install a pen register or a trap and trace device, to exclude "any information that may disclose the physical location of the subscriber . . . ."[60] This exclusion suggests that to obtain cell site data, law enforcement must obtain something more than a court order based merely on a certification that the information sought "is relevant to an ongoing criminal investigation."

IV. Federal Treatment of Citizens' Privacy and Search Interests in Cell Phone Location Tracking

A. United States Supreme Court Cases

As with all discussions of an individual's right of privacy and whether a search was unreasonable, this analysis begins with Justice Harlan's famous test from his concurrence in *Katz v. United States*,[61] commonly referred to as the "*Katz* test." In *Katz*, the Court held that the warrantless use of an eavesdropping device that picked up only sound waves that reached the exterior of a phone booth constituted an unreasonable search under the Fourth Amendment because Katz "justifiably relied" on the privacy of the telephone booth.[62] Harlan wrote that for a privacy interest to exist under the Fourth Amendment, (1) the person must have a subjective expectation of privacy and (2) society must be willing to recognize her subjective expectation as objectively reasonable.[63] The *Katz* test has become the controlling standard for determining whether an individual has a constitutionally protected privacy interest, and if so, whether a search of that interest was unreasonable. Without a warrant, a search of a constitutionally protected privacy interest is "presumptively unreasonable."[64]

57. *See id.* at § 3123(d)(2).
58. 18 U.S.C. § 3123(a)(1), (2).
59. 47 U.S.C. § 1002(a)(2).
60. *Id.* at § 1002(a)(2)(B).
61. *Katz*, 389 U.S. 347.
62. *Id.* at 353, 359.
63. *Id.* at 361 (Harlan, J., concurring).
64. *Id.*

The privacy interest in cell phone location tracking information can be framed in two ways. The first way is whether an individual has a subjective expectation of privacy in the cell phone records that are held by a third-party service provider, and if so, whether society is willing to recognize that expectation as reasonable. The second way it can be framed is whether an individual has an expectation of privacy in his or her location, and if so, whether society is willing to recognize that interest as reasonable. As to the first question—whether one has a privacy interest in records held by a third party—the answer depends on the jurisprudence of the jurisdiction in which the individual is located. The courts' answer to the second question thus far has been "no," finding that society is not willing to recognize an individual's expectation of privacy in his or her location as reasonable.

The United States Supreme Court has considered both questions. In *Smith v. Maryland*,[65] the Court determined that a person does not have an objectively reasonable expectation of privacy in the records held by a third-party service provider. The Court considered whether law enforcement's warrantless use of a pen register was presumptively unreasonable.[66] Borrowing the assumption of the risk doctrine from tort law, the Court held that by dialing a number the subscriber knows will be recorded by the third-party service provider, the caller assumes the risk that the service provider will give this information to law enforcement.[67]

In *United States v. Knotts*,[68] the Court held that a person does not have a reasonable expectation of privacy in his or her location when in plain view on public roads. In *Knotts*, law enforcement placed an electronic tracking beeper inside a container of choloroform.[69] Law enforcement tracked the suspect's movements initially with both visual and tracking beeper surveillance.[70] Officers eventually lost sight of the suspect, and the beeper alone led them to a cabin where they found suspects operating a clandestine lab.[71] The Court held that monitoring the beeper was not an unreasonable search and that the suspect had no right to privacy on the open roads because both the car and the occupants were in plain view.[72] The Court further held that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this

65. *Smith v. Md.*, 442 U.S. 735 (1979).

66. *Id.* at 741–742.

67. *Id.* at 744–745.

68. *U.S. v. Knotts*, 460 U.S. 276 (1983).

69. *Id.* at 278.

70. *Id.*

71. *Id.* at 278–279.

72. *Id.* at 281–282.

case."[73] The Court's rationale for this holding rested on the fact that although law enforcement officers lost sight of the suspect, they would have been able to determine the cabin's location through visual observation had they maintained the surveillance.[74]

In *United States v. Karo*,[75] however, the Court held a similar search to be unreasonable and in violation of the Fourth Amendment.[76] A tracking beeper placed inside a container of ether was used to locate the container inside the suspect's house.[77] The Court's rationale for distinguishing this case from *Knotts* rested on the location of the bucket within the house, which could not have been visually verified from outside.[78] In *Knotts*, on the other hand, the cabin's location could be visually verified by following the car, and law enforcement did not monitor the beeper while the can containing the beeper was inside the cabin.[79]

Cell phone location tracking can be distinguished from *Smith* because most callers do not understand that their cell phone providers are recording and storing their cell site data, let alone that cell phone providers can actually identify their exact locations. Callers cannot "assume the risk" of something they do not even know is happening. As in *Karo*, officers cannot tell whether the tracking device, in this case a cell phone, is or is not inside a home since most people carry them in their pocket, purse, or someplace similar. Even visual observation of a suspect does not allow officers to determine whether the cell phone is within the sanctity of the home. Warrantless tracking of a person's cell phone only while the possessor is outside of a home or private place would require personal surveillance. If the officer must personally watch the suspect to determine when he is in his home, it defeats the point of cell phone location tracking.

Karo and *Knotts* can be compared to cell phone location tracking because the person with the phone is the person about whom law enforcement seeks information, just as the suspects who possessed the containers in *Karo* and *Knotts* were the people about whom law enforcement sought information. The only way for law enforcement to obtain this location information about the suspect is to track the "container" that is linked to the suspect, in this case, a cell phone. Since cell phones are small, they can be concealed much more easily than a container of ether or chloroform. Therefore, when the possessor of the phone goes into his home, as the container did in *Karo*, law enforcement cannot know that fact without the

73. *Id.* at 282.
74. *Knotts*, 460 U.S. at 285.
75. *U.S. v. Karo*, 468 U.S. 705 (1984).
76. *Id.* at 714.
77. *Id.* at 708–710.
78. *Id.* at 714.
79. *Id.* at 713–715.

help of visual observation. Even then, law enforcement might not be able to tell if the cell phone is inside the house or, for example, in a car parked in the driveway.

Obtaining a search warrant based on probable cause would be the most prudent method for obtaining this information for both the police and the public. That way, the prosecutor avoids the risk of having the evidence suppressed as in *Karo*. Securing a warrant also protects the public because a neutral judiciary is making the determination rather than an officer who is personally involved.

B. Federal Circuit and District Court Cases

United States v. Forest,[80] decided by the Sixth Circuit in 2004, is currently the only federal Court of Appeals case examining the subject of cell phone location tracking. In *Forest*, defendants Forest and Garner appealed their convictions for conspiring to distribute cocaine by arguing "the government violated their statutory and constitutional rights by intercepting cell phone data that revealed their location while they were traveling on public highways."[81] DEA agents obtained district court authorization to intercept communications on the defendants' cell phones.[82] These orders also required the service provider, Sprint, to disclose all "subscriber information, toll records, and other information relevant to the government's investigation."[83] The agents attempted to keep visual contact but were not always able to do so. Consequently, one of the agents called Garner's cell phone throughout the day without allowing it to ring on Garner's end. The agents then used Sprint's computer data to determine which towers were receiving signals from Garner's phone, thereby giving them Garner's general location.[84]

Garner argued that evidence against him should have been suppressed because "the DEA's use of cell site data effectively turned his cell phone into a tracking device, violating his rights under both Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2110–2522, and the Fourth Amendment to the United States Constitution."[85] The court held correctly that the cell site data did not constitute "electronic communications."[86] Because the records did not constitute "electronic communica-

80. *Forest*, 355 F.3d 942.

81. *Id.* at 946.

82. *Id.* at 947.

83. *Id.*

84. *Id.*

85. *Id.* at 948. This statute is Title III of the Wiretap Act.

86. *See supra* n. 40–43 and accompanying text for a more detailed explanation of why cell phone location tracking is not considered "electronic communication" under 18 U.S.C. § 2510(12).

tions," the suppression remedies available under the Wiretap Act did not apply. The court noted that assuming the defendant's phone was a "tracking device" under 18 U.S.C. § 3117 (Title I of the ECPA), *United States v. Gbemisola* was persuasive in its holding that § 3117 does not provide any suppression remedies.[87]

The *Forest* court then addressed Garner's Fourth Amendment argument. Because Garner had been tracked only while on public highways, the court concluded that *Knotts* controlled and Garner had no "expectation of privacy in the cell site data because the DEA agents could have obtained the same information by following Garner's car."[88] The court reiterated that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case," which is exactly what the DEA did with the cell site data.[89]

Garner then argued that *Knotts* was distinguishable because the beeper in *Knotts* was government-owned, unlike the cell site data, and that his contract with Sprint did not authorize disclosure of cell site data.[90] Garner also argued that unlike in *Smith*, he did not voluntarily convey his cell site data because he was not dialing out; the DEA was dialing his number. In contrast, Garner argued, Smith had voluntarily conveyed the numbers he dialed himself.[91] The court dismissed these arguments. Because Garner was on a public highway, he had no legitimate expectation of privacy and, therefore, the agent's actions were not a search within the meaning of the Fourth Amendment.[92] With no search under the Fourth Amendment, no Fourth Amendment exclusion remedies were available to Garner.

Though *Forest* is the only Court of Appeals case addressing cell phone location tracking, several federal district courts have considered the issue. Prior to 2005, federal district courts granted requests routinely for cell site data under the authority of the Pen Register Act, SCA, or the Wiretap Act.[93] In August 2005, Magistrate Judge Orenstein "upset the apple cart" with his revolutionary holding in *New York I*.[94] He stated that although he had rou-

87. *Forest*, 355 U.S. at 949–950 (citing *Gbemisola*, 225 F.3d at 758); *see supra* n. 34, regarding *Gbemisola*.

88. *Forest*, 355 U.S. at 951.

89. *Id.* (quoting *Knotts*, 460 U.S. at 282).

90. *Id.*

91. *Id.*

92. *Id.* at 951–952.

93. Samuel, *supra* n. 22, at 1328. *See also In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d 562, 563, 566 (E.D.N.Y. 2005), *on reconsideration sub nom. In re Application of the U.S. for an Or. (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (stating that although other jurisdictions have resolved this issue, no case law on point exists for examination).

94. Samuel, *supra* n. 22, at 1328.

tinely granted applications for cell site data in the past without questioning the legal basis, he denied the current application because correcting that mistake now was better than allowing that flawed practice to continue in the future.[95]

In *New York I*, the government requested cell site data under the SCA, which only requires "specific and articulable facts" showing that the "electronic communication" is "relevant and material to an ongoing criminal investigation."[96] Judge Orenstein determined that although the requested information might appear to be the contents of an "electronic communication," the definition of electronic communication specifically excludes "tracking devices," and that in this case, the cell phone was used as a tracking device.[97] He therefore denied the application for cell site data under the SCA.[98] Judge Orenstein next analyzed whether the application could be granted under the Pen Register Act.[99] Reading the Act in conjunction with CALEA, he determined that Congress specifically prohibited service providers from giving law enforcement information disclosing the physical location of the subscriber.[100] He held: "In other words, where a carrier's assistance to law enforcement is ordered on the basis of something less than probable cause, such assistance must not include disclosure of a subscriber's physical location."[101]

Two months after *New York I* was decided, in October 2005, Magistrate Judge Smith followed Judge Orenstein with his decision in *Texas I*.[102] He held that prospective cell site data qualifies as tracking device information under Title I of the ECPA and that a probable cause warrant under Federal Rule of Criminal Procedure 41 is the appropriate standard that must be applied.[103] He also held the government may not obtain such data under the Pen Register Act, SCA, or the Wiretap Act by themselves.[104] Further, Judge Smith rejected the Government's hybrid theory in which the SCA is used in conjunction with CALEA and the Pen Register Act as being "little more than a retrospective assemblage of disparate statutory parts to achieve a desired result."[105] He reasoned that "if these various statutory provisions

95. *In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d at 566 (quoting *Henslee v. Union Planters Nat. Bank & Trust Co.*, 335 U.S. 595, 600 (1949) (Frankfurter, J., dissenting) ("Wisdom too often never comes, and so one ought not to reject it merely because it comes late.")).

96. *Id.* at 563.

97. *Id.* at 564.

98. *Id.*

99. *Id.* at 565.

100. *Id.*

101. *In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d at 563.

102. *Application for Pen Register*, 396 F. Supp. 2d at 747.

103. *Id.* at 752.

104. *Id.* at 757.

105. *Id.* at 765.

were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way."[106] He also noted that law enforcement efforts would not be hindered by this decision because law enforcement could always apply for a warrant under the Rule 41 probable cause standard.[107]

Since these decisions in 2005, many other federal cases have been decided with mixed results.[108] Some courts have held that probable cause is required under the law; others that a lesser standard is adequate. Even though the United States Supreme Court and federal district courts have stated that nothing in Fourth Amendment jurisprudence stops officers from augmenting their natural senses, this outcome could be different under Montana constitutional law. Although Montana courts may find guidance in looking to the limited federal law on the issue of cell phone location tracking, they also have the additional guidance of Article II, § 10 of the 1972 Montana Constitution—Montana citizens' explicit right of privacy—as well as Article II, § 11—Montana citizens' right to be free from unreasonable searches and seizures.

V. Cell Phone Location Tracking under Montana Law

A. 1972 Constitutional Convention

Article II, § 10 of the Montana Constitution provides: "The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest." The 1972 Constitutional Convention delegates put much thought into this provision. The delegates included this provision because of concerns about government surveillance of Montana citizens and the increasing sophistication

106. *Id.* at 764.

107. *Id.* at 765.

108. *See In re Application of the U.S. for an Or. Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134 (D.D.C. 2006); *In re the Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re the Application of the U.S. for an Or. Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. under 18 U.S.C. 2703*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In re the Application of the U.S. for an Or. Authorizing the Installation & Use of a Pen Register with Caller Identification Device & Cell Site Location Authority on a Certain Cellular Tel.*, 415 F. Supp. 2d 663 (S.D.W. Va. 2006); *In re Application of the U.S. for Or. Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. (Sealed)*, 416 F. Supp. 2d 390 (D. Md. 2006); *In re Application of the U.S. for an Or.: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info.*, 411 F. Supp. 2d 678 (W.D. La. 2006); *In re Application of the U.S. for an Or.: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info.*, 433 F. Supp. 2d 804 (S.D. Tex. 2006).

of surveillance mechanisms.[109] Delegate Robert Campbell believed that participating members of society understand the State must intrude into their private lives at times, but the State should not do so unless it has "a good reason for being there."[110] He stated that including an explicit right of privacy would "guarantee our individual citizens of Montana this very important right—the right to be let alone; and this has been called the most important right of them all."[111]

Delegate Campbell explained the purpose of including Article II, § 10 when he read from a February 3, 1972, *Montana Standard* article. The quotation illustrates the concerns that led the delegates to insert an individual privacy provision in the newly crafted constitution:

> Times change. That in a nutshell, is why the Constitutional Convention delegates in Helena are working on a new and more modern governmental charter for Montana. Today, with wiretaps, electronic and bugging devices, photo surveillance equipment and computerized data banks, a person's privacy can be invaded without his knowledge and the information so gained can be misused in the most insidious ways. It isn't only a careless government that has this power to pry; political organizations, private information gathering firms, and even an individual can now snoop more easily and more effectively than ever before. We certainly hope that such snooping is not as widespread as some persons would have us believe, but with technology easily available and becoming more refined all the time, prudent safeguards against the misuses of such technology are needed. Some may urge and argue that this is a legislative, not a constitutional issue. We think the right of privacy is like a number of other inalienable rights; a carefully worded constitutional article reaffirming this right is desirable. Wade Dahood of Anaconda, Chairman of the Bill of Rights Committee, hit the nail on the head when he said: "As government functions and controls expand, it is necessary to expand the rights of the individual." The right to privacy deserves specific protection.[112]

Several delegates strongly voiced their distaste for the use of electronic surveillance in Montana. Delegate Mae Nan Robinson stated that she believed "there is certainly no justification for [electronic surveillance] in this state" and that "no case has been or can be made for wiretapping in the State of Montana, to have such a blatant disregard of privacy of individuals."[113] She further stated that privacy and wiretapping, or other electronic surveillance, were "probably [the] two most incompatible things that you could ever have."[114] Delegate David Holland agreed and stated he "support[ed] the position that there should be no wiretapping or other electronic

109. *Montana Constitutional Convention Proceedings* vol. 5, 1680–1688, 1850–1853 (Mont. Legis. & Legis. Council 1972) (available at http://courts.mt.gov/library/montana_laws.mcpx).

110. *Id.* at vol. 5, 1681.

111. *Id.*

112. *Id.*

113. *Id.* at vol. 5, 1683, 1684.

114. *Id.* at 1683.

surveillance . . . ."[115] Perhaps the most powerful statement of distaste for governmental wiretapping and electronic surveillance came from the mouth of the Chairman of the Bill of Rights Committee, Delegate Wade Dahood. He stated:

> [I]t is inconceivable to any of us that there would ever exist a situation in the State of Montana where electronic surveillance could be justified. And the thinking throughout the United States is, electronic surveillance shall be justified only in matters involving national security, perhaps in matters involving certain heinous federal crimes where the situation is such that in those instances we must risk the right of individual privacy because there is a greater purpose to be served. But within the area of the State of Montana, we cannot conceive of a situation where we could ever permit electronic surveillance . . . we would not object to allow[ing] an amendment that would prohibit electronic surveillance in the State of Montana.[116]

Although such an amendment was never added, the delegates' intention was clear—they wanted to protect Montanans' privacy interests against electronic surveillance as vigorously as they could. For instance, at one point in the discussion, the delegates removed the phrase "without the showing of a compelling state interest" from the language of Article II, § 10 so that it read: "The right of individual privacy is essential to the well-being of a free society and shall not be infringed."[117] This was done to "let [the] statement about right of privacy simply stand just right there, barefaced, on its own; that we have the right to privacy as stated" and out of fear that the additional phrase "may be interpreted by whatever state agency happens to have an interest in invading my privacy at that particular time."[118] The phrase was eventually reinserted after several delegates voiced their concerns that its deletion might actually weaken the clause because, without strict guidance, courts might interpret Article II, § 10 in a manner the delegates did not intend. Delegate Thomas Ask summed up the delegates' rationale for reinserting the compelling state interest language:

> By putting these words in, we're giving direction to the court how they are going to interpret this. If there's no compelling state interest, you can't invade a person's right of privacy . . . so we [need to reinsert the original language to] clarify this issue and [not] cloud it up and create a legal hassle in the years to come.[119]

After the delegates unanimously passed Article II, § 10, they moved on to debate Article II, § 11, the Montana Constitution's search and seizure provision:

---

115. *Montana Constitutional Convention Proceedings*, *supra* n. 109, at vol. 5, 1683.

116. *Id.* at vol. 5, 1687.

117. *Id.* at vol. 5, 1681–1682.

118. *Id.* at vol. 5, 1682.

119. *Id.* at vol. 5, 1850–1851.

> The people shall be secure in their persons, papers, homes and effects from unreasonable searches and seizures, and no warrant to search any place or seize any person or thing shall issue without describing the place to be searched or the person or thing to be seized, nor without probable cause, supported by oath or affirmation, reduced to writing.

Delegate Campbell was the first to comment during the discussion of Article II, § 11, and he spoke again about the delegates' intent to protect Montanans from electronic surveillance:

> You may note that in our rough draft when we did present it to the Convention, it did contain specific information regarding electronic equipment and surveillance. We at the committee felt very strongly that the people of Montana should be protected as much as possible against eavesdropping, electronic surveillance, and such type of activities. We also recognize that there may in the future be a legitimate need for such in legitimate police activities. After careful consideration of the rough draft that we did produce, we found that the citizens of Montana are very suspicious of such type of activity. We found from the law enforcement officers we talked to that there was really not a need and such activity was not taking place at this time.[120]

The specific language about electronic equipment and surveillance was not included in the final version because the delegates recognized that law enforcement might someday have a legitimate reason for using this technology, and the Legislature could deal with it at that time.[121] The delegates, however, did not leave the matter at that. Delegate Campbell expressed the Bill of Rights Committee's intent that Article II, § 11 be read in conjunction with Article II, § 10, thereby giving citizens broad protection against unreasonable searches and seizures.[122]

Although law enforcement informed the delegates that the activities they were concerned about were not going on at the time, those activities are certainly going on today. The delegates' forward-looking discussions, thoughts, and protections were implemented for the purpose of protecting Montanans from the always improving technology that may one day invade the search, seizure, and privacy rights of Montanans. The delegates' clear intent supports the argument that the government must have a compelling state interest before it may use cell phone location tracking technology. The Montana Supreme Court often looks to the transcripts of the 1972 Constitutional Convention for guidance on how to interpret constitutional provisions and has done so when interpreting Montanans' right to privacy and right to be free from unreasonable searches and seizures on many occasions. With that as a foundation, this article will now examine Montana's case law on the subject of cell phone location tracking.

---

120. *Id.* at vol. 5, 1683.

121. *Montana Constitutional Convention Proceedings*, *supra* n. 109, at vol. 5, 1683.

122. *Id.*

B. Montana Case Law

The Montana Supreme Court subscribes to the philosophy that state courts are free to provide citizens greater rights and protections under state constitutions than the federal Constitution provides, even if the language is identical. For instance, the Montana Supreme Court has stated: "Independent state grounds exist for this Court to extend greater privacy rights, and thereby greater protection against unreasonable search and seizure, than would be afforded under the Federal Constitution."[123] The independent state ground referred to by the Court is the Montana Constitution's explicit right of privacy in Article II, § 10.[124] Moreover, Montana's Supreme Court firmly adheres to the principle that it will not "march lockstep" with the United States Supreme Court because of this independent state ground for providing broader protections than those provided by the United States Constitution.[125] By recognizing that the Montana Constitution's right of privacy is to be read in conjunction with the Montana Constitution's right against unreasonable searches and seizures, the Court has honored the intent of the delegates. The Court has repeatedly reaffirmed that "the right to privacy is the cornerstone of protections against unreasonable searches and seizures."[126]

The Court has recognized that two types of privacy interests exist under the Montana Constitution: informational privacy and autonomy privacy. Informational privacy has been defined as an "interest[ ] in precluding the dissemination or misuse of sensitive and confidential information."[127] Autonomy privacy has been defined as "the interest[ ] in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference."[128] The Court analyzes these two privacy rights somewhat differently. Because informational privacy fits this situation best—the government accesses cell site data that is held in phone records generated by the service provider—autonomy privacy will not be discussed further. Informational privacy will be examined in the context of

123. *State v. Solis*, 693 P.2d 518, 521 (Mont. 1984), *rev'd in part on other grounds, State v. Goetz*, 191 P.3d 489, 497 (Mont. 2008).

124. *Id.* at 520–521.

125. *State v. Bullock*, 901 P.2d 61, 70, 72, 74, 75 (Mont. 1995); *State v. Siegal*, 934 P.2d 176, 191 (Mont. 1997), *rev'd in part on other grounds, State v. Kuneff*, 970 P.2d 556 (Mont. 1998); *Solis*, 693 P.2d at 521; *State v. Nelson*, 941 P.2d 441, 447 (Mont. 1997) (citations omitted); *Goetz*, 191 P.3d at 496–497. *Goetz* overruled *State v. Brown*, 755 P.2d 1364 (Mont. 1988), because *Brown* was decided by federal analysis without consideration of Montana's heightened right of privacy. *Goetz*, 191 P.3d at 496–497.

126. *Siegal*, 934 P.2d at 191 (citing *Solis*, 693 P.2d at 522–523).

127. *Nelson*, 941 P.2d at 448 (citing *Hill v. Natl. Collegiate Athletic Assoc.*, 865 P.2d 633, 654 (Cal. 1994)).

128. *Id.*

whether a search has occurred when the government seeks to obtain the subscriber's cell phone records and cell site data from the service provider.

A search is defined as "the use of some means of gathering evidence which infringes upon a person's reasonable expectation of privacy."[129] Montana uses the "*Goetz* test," a three-pronged analysis similar to the *Katz* test, to determine if a search has been conducted. Under the *Goetz* test, the Court determines the following: (1) Does the person challenging the state's action have an actual subjective expectation of privacy? (2) Is Montana society[130] willing to recognize that subjective expectation as objectively reasonable? and (3) What is the nature of the state's intrusion?[131]

To decide whether a person has a subjective expectation of privacy, the Court looks at the particular circumstances of each case and decides if the person has "knowingly exposed something to the public," thereby surrendering his or her privacy protections.[132] To determine whether the second prong has been met, the Court examines the underlying constitutional values "including respect for *both* private, subjective expectations and public norms."[133] In a case involving the constitutionality of technologically enhanced government surveillance, the Court will "identify the values at risk, and vest the reasonable expectation of privacy test with those values."[134]

Finally, to determine if the nature of the State's intrusion was valid, the Court reads Article II, §§ 10 and 11 in conjunction. The Court first examines whether the procedural safeguards of a probable cause warrant or a warrant exception have been met under § 11; it then determines whether the State has shown a compelling state interest as required by Article II, § 10.[135] The purpose of reading the two provisions together is to ensure that "an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals."[136] A compelling state interest exists where the State is enforcing its criminal laws to benefit and protect the fundamental rights of its citizens. This enforcement must also be tailored closely to effectuate only that compelling interest.[137] Where the State can show probable cause

129. *State v. Cotterell*, 198 P.3d 254, 263 (Mont. 2008) (citations omitted).

130. *See Bullock*, 901 P.2d at 76 ("which the society of *this State* is willing to recognize as reasonable") (emphasis added).

131. *Goetz*, 191 P.3d at 497–498.

132. *Id.* at 498 (citing *State v. Scheetz*, 950 P.2d 722, 726–727 (Mont. 1997)).

133. *Goetz*, 191 P.3d at 499 (emphasis in original) (citation omitted).

134. *Id.*

135. *Id.* at 500–501.

136. *Id.* at 501.

137. *Solis*, 693 P.2d at 522 (citations omitted); *Siegal*, 934 P.2d at 184 (citing *State v. Pastos*, 887 P.2d 199, 202 (Mont. 1994)).

that a crime has been committed and that information relating to the commission of the crime is in possession of a certain person or institution, it has shown a compelling state interest.[138] The issue in an informational privacy and search analysis in the cell site data context is whether a cell phone subscriber has an actual, subjective expectation in cell phone records held by a third-party service provider.

In Montana, the examination of privacy rights in information held by third-party service providers has been limited to billing records. In *Hastetter v. Behan*, the plaintiff sued an employee of a phone company under Article II, § 10 for looking at the numbers the plaintiff dialed on his landline telephone without the plaintiff's consent or knowledge.[139] This case did not involve a government actor or a request by the government for the information.[140] The Montana Supreme Court held in *Hastetter* that "telephone billing records are not private matters because the public awareness that such records are routinely maintained negates any constitutional expectation of privacy regarding the records."[141]

The Court's analysis of privacy expectations for landline phone billing records in *Hastetter* does not apply to cell phone location tracking for several reasons. First, because *Hastetter* involved private parties, no state action was involved; therefore, Article II, § 11 was not implicated. In the case of cell phone location tracking, a state actor would be the one obtaining the cell phone records containing the cell site data, thereby implicating an analysis under Article II, § 11 as well as § 10. Second, when law enforcement looks at a billing record to see the numbers that have been dialed, any location data, such as an area code, is merely incidental. When law enforcement looks at the cell phone records containing location data to track the person with the phone, it is looking at the records for the *very purpose* of obtaining location data; the location data is not merely incidental.[142] Tracking a person's exact location provides law enforcement with information that is more intrusive and personal in nature than merely looking at the numbers dialed on a phone. Third, landline records are more general than cell phone records because the information generated by landlines, which are typically in homes or businesses, provides information about everyone who uses the landline in the home or the business. Conversely, cell phones are typically carried by only one person, meaning the records are much more personal.

---

138. *Nelson*, 941 P.2d at 449.

139. *Hastetter v. Behan*, 639 P.2d 510, 511 (Mont. 1982).

140. *Id.*

141. *Id.* at 513.

142. *See* McLaughlin, *supra* n. 8, at 434–435 (using a similar analysis when discussing federal use of pen registers rather than cell phone location tracking).

Additionally, billing records from a landline cannot pinpoint a person's exact location unless he is in his home making or receiving a call because there are no registration signals generating cell site data that can be triangulated. Landline telephones are associated with an address, so any time a landline is used, the caller is at that address. Unlike a cell phone, however, the landline does not follow the caller where he or she goes because it is attached to land; therefore, the information that can be gleaned from a cell phone can be much more personal to the caller than information gleaned from a landline. Even with the advent of "caller ID" with landline phones, the only location data that is provided is incidental because, much like a pen register, it only records the *numbers* of the incoming calls—not the actual cell site data from cell phone towers that shows the caller's exact location.

Finally, whereas the *Hastetter* Court held that a person gives up his right to privacy because he knows the phone company is recording the numbers dialed, most people do not know that their phones are broadcasting registration signals every seven seconds, let alone that the service provider is keeping this information. Because most subscribers have no knowledge that the cell site data is being stored by their service providers, they cannot be said to have voluntarily waived their constitutional expectation of privacy in those records. This analysis may change as people become more aware of cell phone technologies and capabilities.

The next inquiry becomes whether, by looking at the facts of the case, the subscriber "knowingly exposed something to the public and, consequently, surrendered his . . . privacy protections" when the records are held by the third-party service provider.[143] As stated above, most people do not know that the registration process is even happening or that registration and the calls they make or receive are generating records that contain information that can pinpoint their location. Because people are oblivious to the fact that their location data is being generated and recorded every seven seconds, they cannot be said to have "knowingly" exposed anything. Also, what they do knowingly expose, such as the numbers they dial, is not being exposed to the public—it is being exposed to their service provider with whom they likely have a contract. Again, this analysis will change as people's knowledge about cell phone technology increases. In the meantime, practitioners will need to read the individual contracts their clients have with the respective service providers to ascertain whether they contain any provisions regarding privacy or the release of information to third parties.

The hypothetical cell phone subscriber has not knowingly exposed his cell site data, and he has certainly not exposed his cell site data to the pub-

143. *Goetz*, 191 P.3d at 498 (citing *Scheetz*, 950 P.2d at 726–727).

lic—only to his service provider. Because he has not "knowingly exposed something to the public," he cannot be said to have "surrendered his . . . privacy protections." He, therefore, has a subjective expectation of privacy in his cell phone records held by the third-party service provider.

To determine whether Montana society recognizes a subjective expectation of privacy as objectively reasonable, the Court looks to the underlying values, "including respect for *both* private, subjective expectations and public norms."[144] Also, when dealing with "technologically enhanced government surveillance," the Court will identify the values at risk and "vest the reasonable expectation of privacy test with those values."[145] The Court takes seriously the intent of the delegates in framing that right.[146] Moreover, the right against unreasonable searches and seizures "protects people not places,"[147] and "what an individual seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[148]

The Montana Supreme Court has frequently provided stronger protections under the Montana Constitution than are provided at the federal level. In *Goetz*, the Court held that Montanans would find objectively reasonable the defendant's subjective expectation that the government would not record his conversations without his knowledge, reiterating: "Montanans still continue to cherish the privacy guaranteed them by Montana's Constitution."[149] In *Siegal*, law enforcement conducted a warrantless scan of the defendant's house with a thermal imager.[150] Holding that this was an unreasonable search, the Court quoted the delegates' strong distaste for electronic surveillance by the government and commented that Montanans would be "shocked and consider it a gross invasion of their privacy" to find that the government was scanning their homes with a thermal imager without a warrant or their consent.[151]

The constitutional convention delegates' extensive discussion about their disgust for electronic monitoring and surveillance demonstrates that this is not a newly held belief by Montanans and is in fact the very reason why the delegates thought including an explicit right to individual privacy in the 1972 Montana Constitution was necessary. Because of these beliefs, Montanans reasonably expect that the government will not snoop around in

144. *Goetz*, 191 P.3d at 499 (emphasis in original) (citation omitted).

145. *Id.*

146. *See Siegal*, 934 P.2d at 184, 190; *Goetz*, 191 P.3d at 499–500; *Bullock*, 901 P.2d at 75 ("Montana has a strong tradition of respect for the right to individual privacy."); *Solis*, 693 P.2d at 521–522 (quoting the Constitutional Convention transcripts extensively).

147. *Bullock*, 901 P.2d at 70.

148. *Id.* (citing *Katz*, 389 U.S. at 351).

149. *Goetz*, 191 P.3d at 500.

150. *Siegal*, 934 P.2d at 178.

151. *Id.* at 190–191.

their cell phone records to spy on their locations without their knowledge. Furthermore, Article II, § 11 protects the privacy interests that society would deem reasonable, not the location in which those privacy interests are kept. Thus, it protects a person's interest in his cell phone records, not the records facility of a third-party service provider. Because the records are "what an individual seeks to preserve as private," the records "may be constitutionally protected"[152] if the third prong of the privacy test can also be met. For these reasons, Montana society would find the hypothetical phone subscriber's subjective expectation to privacy in his cell phone records held by the third-party service provider to be objectively reasonable.

The inquiry into the nature of the State's intrusion seeks to ensure that the safeguards of Article II, § 11 have been met.[153] Article II, § 11 requires either the State to obtain a warrant based on probable cause or the search to fit a recognized warrant exception.[154] Probable cause exists "when facts and circumstances presented to a magistrate would warrant an honest belief in the mind of a reasonable and prudent person that an offense has been, or is being, committed and that property (or information) sought exists at the place designated."[155] The warrant requirement is necessary "so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals."[156]

Whether probable cause or a warrant exception exists would depend on the facts of the case at issue. For example, a court would likely find the search reasonable if the government searched a suspect's cell phone location data after obtaining a warrant in order to corroborate an alibi. Although the subscriber would have an objectively reasonable expectation of privacy, the State would have a compelling state interest in protecting other members of society and solving a crime. Further, it would have the necessary procedural safeguard of a neutral magistrate granting a search warrant based on probable cause. However, if the government were conducting random checks on citizens to see what they had been up to without "a good reason for being there," as Delegate Campbell said, such a search likely would not pass muster under the Montana Constitution.

---

152. *Bullock*, 901 P.2d at 70 (citing *Katz*, 389 U.S. at 351).

153. *Goetz*, 191 P.3d at 500.

154. *Id.* at 500–501.

155. *Nelson*, 941 P.2d at 449 (citing *Siegal*, 934 P.2d at 193).

156. *Goetz*, 191 P.3d at 501.

If cell phone location tracking is analyzed from the angle of informational privacy in the context of a search, the Montana Constitution likely would protect Montanans from warrantless snooping by the government.

VI. Conclusion

Police are still able to use visual surveillance techniques; however, when they lose sight of a suspect or cannot find a suspect to begin with, the police must comply with the demands of the Montana Constitution before obtaining the suspect's cell site data. To ensure the greatest protections for Montanans and honor the intent of the delegates in crafting the 1972 Montana Constitution, the best argument for preventing abuse of cell phone location tracking technology is that it implicates an informational privacy interest under Article II, § 10, read in conjunction with the right against unreasonable search and seizures in Article II, § 11. This argument comports with the established framework of *Goetz*.

Because Montanans still value their right of privacy and their right to be free from unreasonable searches and seizures, the cell phone records that convey Montanans' whereabouts should only be available to law enforcement after a showing of probable cause or with a warrant exception. Tracking someone by using police visual surveillance techniques should be the rule, not the exception. Police officers should not be able to use technology to find someone whom they could not find with good old-fashioned sleuth work, unless they obtain a warrant and show a compelling state interest in invading a person's private records to a neutral judiciary.

As the use of cell phone tracking becomes more prevalent in Montana, the Court or the Legislature may implement a novel standard of review or statutory framework for analyzing this situation or obtaining cell site data. Until then, the *Goetz* test appears to be the best candidate for keeping the rights guaranteed to Montanans under the 1972 Constitution intact, and to address and recognize the forward-looking concerns of the delegates.